Prepared Remarks for U.S. Attorney Preet Bharara
September 30, 2010

Introduction

Good afternoon. My name is Preet Bharara, and I am the United States Attorney for the Southern District of New York.

I have often spoken about the dangers that cybercrime poses to our financial infrastructure. Today, we announce a serious and concrete example of this gathering threat, and our efforts against it. The threat is international, and that is why the response is global.

What you saw yesterday in the United Kingdom *[Metropolitan Police Service]* and what you are seeing today in the United States is part of a sweeping and coordinated effort to combat the 21st century's variation on traditional bank robbery.

As today's arrests show, the modern, high-tech bank heist does not require a gun, a mask, a note, or a getaway car. It requires only the Internet and ingenuity. And it can be accomplished in the blink of an eye, with just a click of the mouse – at a distance of thousands of miles.

As I will describe in a moment, this case involves dozens of defendants who allegedly helped Eastern European hackers steal millions of dollars from U.S. banks with the aid of a malicious computer program that acted as a Trojan horse on unsuspecting computers.

Known internationally as the Zeus Trojan, this software program allegedly allowed criminals to spy on bank customers, steal their account information, and then steal their money.

In all, today we have charged 37 defendants federally for helping to steal more than $3 million from bank accounts compromised by the Zeus software; dozens more have been charged locally by the Manhattan District Attorney.

The victims include five banks, as well as dozens of individual and business account holders throughout the country.

Before I go into the details of the charges, let me introduce the team that got us here:

- I am pleased to be joined by Manhattan District Attorney Cy Vance, whose Office has played an important role in this effort, and who has charged dozens of additional defendants in state court. Today's joint announcement reflects the deep commitment of our two offices to work together to protect citizens from all types of crime. I would like to thank the Assistant District Attorneys from Cy's Office who have worked so hard on these cases:
  - Chief of the Cybercrime and Identity Theft Bureau David Szuchman
  - Deputy Chief of the Cybercrime and Identity Theft Bureau Jeremy Glickman, and
  - Assistant District Attorney Joanne Li

- I am also joined by representatives from law enforcement agencies who have participated in the cases we are announcing today, including:

  - Assistant Director-in-Charge of the New York Office of the FBI Janice Fedarcyk
  - Special Agent-in-Charge of the New York Office of the FBI Austin Berglas
  - Commanding Officer of the Financial Crimes Task Force of the NYPD Gregory Antenson
  - Assistant Special Agent-in-Charge of the New York Office of the Secret Service, Paul Mahon
  - Deputy Special Agent-in-Charge of the NY Office of Homeland Security Investigations Glenn Sorge, and
  - Assistant Special Agent-in-Charge of the NY Office of Diplomatic Security Service Pasquale Capriglione.

I am also joined by members of my Office's Complex Frauds Unit, which oversees our cybercrime enforcement efforts, and is supervising the investigation and prosecution of these cases: Assistant United States Attorneys Joseph Facciponti, Sarah Lai, Andrew Bauer, Tom Brown, and Justin Anderson, along with the chiefs of the Complex Frauds Unit, Jonathan Kolodner and Anirudh Bansal. I'd like to thank them for their careful and thorough investigation of these cases.
You know, exactly one year and one day ago, we established the Unit in order to put greater focus and resources to the investigation and prosecution of large-scale sophisticated frauds and cyber crimes.

The charges we are announcing today are a direct result of this effort and show that we are moving in the right direction to root out cyber crime.

The Scheme

Let me take a few minutes to tell you how the scheme that we've brought down worked, and the roles the defendants allegedly played in the scheme.

[Chart]

The charges unsealed today include bank fraud, money laundering, use of false identification documents and passport fraud.

The digital age brings with it many benefits, but also many challenges for law enforcement and our financial institutions.

Cyber-criminals can cloak their identities with screen names, or, as in this case, attack our infrastructure from abroad with spyware that do the dirty work for them.

They are supported by sophisticated domestic networks with access to false documents, through which they secure their ill-gotten gains.

In short, the last several years have shown that the mouse and the keyboard can be far more effective than the gun and the mask. But today's operation demonstrates that these organizations, wherever they are located, are not anonymous, and are not invulnerable.

Working with our colleagues abroad and locally, we will attack this threat at every level, to make sure that there is no safe haven for the 21st Century bank robber.

- Cy Vance, Manhattan DA
- Janice Fedarcyk, ADIC of FBI in New York
- Deputy Inspector Gregory Antonsen, Commanding Officer of NYPD's Financial Crimes Task Force